УДК 621.391.7

Ю. Є. Яремчук, канд. техн. наук, доц.

МОЖЛИВІСТЬ ФОРМУВАННЯ ТА ПЕРЕВІРКИ ЦИФРОВОГО ПІДПИСУ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

Запропоновано можливість формування та перевірки цифрового підпису на основі математичного апарату рекурентних V_k-послідовностей. Аналіз показав, що в цілому така можливість забезпечує приблизно такий самий рівень криптографічної стійкості та обчислювальної складності, як і відомі аналоги, але при цьому дозволяє змінювати стійкість методу залежно від порядку послідовності, а також має простішу процедуру задання параметрів. За певних умов запропонована можливість цифрового підписування забезпечує значне підвищення швидкості виконання процедури перевірки підпису, а також підвищення стійкості всього процесу цифрового підписування.

Вступ

Електронний цифровий підпис [1—4] використовується для автентифікації даних, що передаються телекомунікаційними каналами, функціонально є аналогом звичайного рукописного підпису і володіє такими його основними властивостями: посвідчує, що підписані дані надходять від особи, яка поставила підпис; не дає можливості підписанту відмовитись від зобов'язань, пов'язаних з підписаними даними; гарантує цілісність підписаних даних.

Цифрові підписи мають широке застосування в галузі інформаційної безпеки, включаючи автентифікацію, цілісність даних і безвідмовність [2]. Одним з найважливіших застосувань цифрового підпису є сертифікація відкритих ключів у великих мережах. Сертифікація забезпечує можливість довіреній третій стороні (TTP — trusted third party) зв'язати ідентичність користувача з відкритим ключем, щоб у подальшому інші користувачі могли перевірити автентичність відкритого ключа без допомоги довіреної третьої сторони.

Першим методом цифрового підписування є схема RSA [5], яка залишається на сьогодні однією з найпрактичніших та універсальних. Подальші дослідження привели до низки альтернативних методів цифрового підписування. Деякі з них мають значні переваги з точки зору функціональності та реалізації, зокрема методи Ель-Гамаля, Шнорра, DSA, ГОСТ 34.10 [2—4]. Ці методи базуються на операції піднесення до степеня, яка вимагає виконання досить складних обчислень, що впливає на швидкість роботи методу під час його практичної реалізації.

В зв'язку з цим певний інтерес викликає апарат на основі рекурентних послідовностей [6], який дозволяє за певних умов спрощувати обчислення під час вирішення криптографічних задач. Так, в роботі [7] описано метод автентифікації сторін взаємодії, який базується на рекурентних V_k-послідовностях і забезпечує спрощення обчислень з боку перевіряльника.

Виходячи з цього, актуальною є розробка методу цифрового підписування на основі рекурентних послідовностей, який би забезпечував спрощення обчислень під час цифрового підписування і при цьому забезпечував достатній рівень криптографічної стійкості.

Можливість цифрового підписування на основі рекурентних V_k-послідовностей

В [6] розглянуто V_k-послідовність, яка складається з V_k^+-послідовності та V_k^--послідовності.

V_k^+-послідовністю називається послідовність чисел, що обчислюються за формулою

$$v_{n,k} = g_k v_{n-1,k} + g_1 v_{n-k,k} \tag{1}$$

для початкових значень $v_{0,k} = 1$, $v_{1,k} = g_2$, коли $k = 2$; $v_{0,k} = v_{1,k} = ... = v_{k-3,k} = 0$, $v_{k-2,k} = 1$, $v_{k-1,k} = g_k$, коли $k > 2$, де g_1, g_k — цілі числа; n і k — цілі додатні.

Обчислення елементів цієї послідовності для спадних n, починаючи з деякого значення $n = l$, буде здійснюватись таким чином:

$$v_{n,k} = \frac{v_{n+k,k} - g_k \cdot v_{n+k-1,k}}{g_1}. \quad (2)$$

V_k^--послідовністю називається послідовність чисел, що обчислюються за формулою (5) для n від'ємних за початкових значень $v_{-1,k} = 0$, $v_{-2,k} = g_1^{-1}$ для $k = 2$; $v_{-1,k} = 0$, $v_{-2,k} = g_1^{-1}$, $v_{-3,k} = v_{-4,k} = ... = v_{-k,k} = 0$ для $k > 2$.

Для будь-яких цілих додатних n, m та k отримано таку аналітичну залежність [6]:

$$v_{n+m,k} = v_{m+(k-2),k} \cdot v_{n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{m+(k-2)-i,k} \cdot v_{n-k+i,k}. \quad (3)$$

Для будь-яких цілих додатних n і m, таких що $1 \le m < n$ та будь-якого цілого додатного k існує така залежність [6]:

$$v_{n-m,k} = v_{-m+(k-2),k} \cdot v_{n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{-m+(k-2)-i,k} \cdot v_{n-k+i,k}. \quad (4)$$

Подані рекурентні послідовності, а також отримані залежності дозволяють запропонувати таку можливість цифрового підписування на їх основі.

Суть можливості цифрового підписування, що пропонується (заявка на корисну модель № u 2013 06325 від 22.05.2013 р.), базується на використанні властивості (3) V_k-послідовності, яка дозволяє використовувати її для обчислення елемента $v_{n+m,k}$, а також для обчислення елемента $v_{-n+m,k}$. Крім того властивість (3) дозволяє реалізувати процедуру обчислення елемента $v_{n \cdot m,k}$. Так само на основі властивості (4) можна реалізувати процедуру обчислення елемента $v_{-n \cdot m,k}$. Все це дає можливість створення такого методу цифрового підписування.

Спочатку відправник-підписант (або центр довіри) виконує попередню процедуру вибору параметрів та обчислення ключів. При цьому він випадковим чином вибирає секретний ключ a, за допомогою якого обчислює, а потім передає одержувачу-перевіряльнику відкритий ключ $v_{-a+i,k}$, $i = \overline{-k,-1}$.

В процесі формування цифрового підпису для повідомлення M відправник-підписант вибирає випадкове число b, обчислює $v_{b,k}$, визначає значення x як $x = v_{b,k}$ та обчислює значення r як $r = \left(h(M) \cdot x\right) \bmod p$ за допомогою обраної функції хешування h від повідомлення M. Далі він визначає значення s як $s = b + a \cdot r$. Після цього отриману множину цілих чисел $\{r; s\}$ він перетворює у цифровий підпис вигляду $DS = \left(0 \| r \| 0 \| s\right)$ і передає його разом з повідомленням M одержувачу.

Перевіряючи цифровий підпис, одержувач спочатку обчислює $v_{-a \cdot r+i,k}$, $i = \overline{-(k-1),0}$, на основі відкритого ключа — елементів $v_{-a+i,k}$, $i = \overline{-k,k-2}$, та отриманого від підписанта значення r, а потім на основі обчислених щойно елементів та отриманого від підписанта значення s він обчислює елементи $v_{s+i,k}$, $i = \overline{-1,k-2}$.

Після цього на основі усіх обчислених підписантом елементів він обчислює значення x' як $x' = v_{-a \cdot r+s,k}$, використовуючи залежність (3), а потім обчислює значення r' як $r' = \left(h(M) \cdot x'\right) \bmod p$ та перевіряє, чи виконується $r \stackrel{?}{=} r'$. Якщо так, то підпис приймається, в іншому випадку — відкидається.

Не важко пересвідчитись, що для підпису, згенерованого згідно з цим методом, перевірка $r \stackrel{?}{=} r'$ завжди буде виконуватись.

Виходячи з цього, схема цифрового підписування буде мати такий вигляд (рис.).

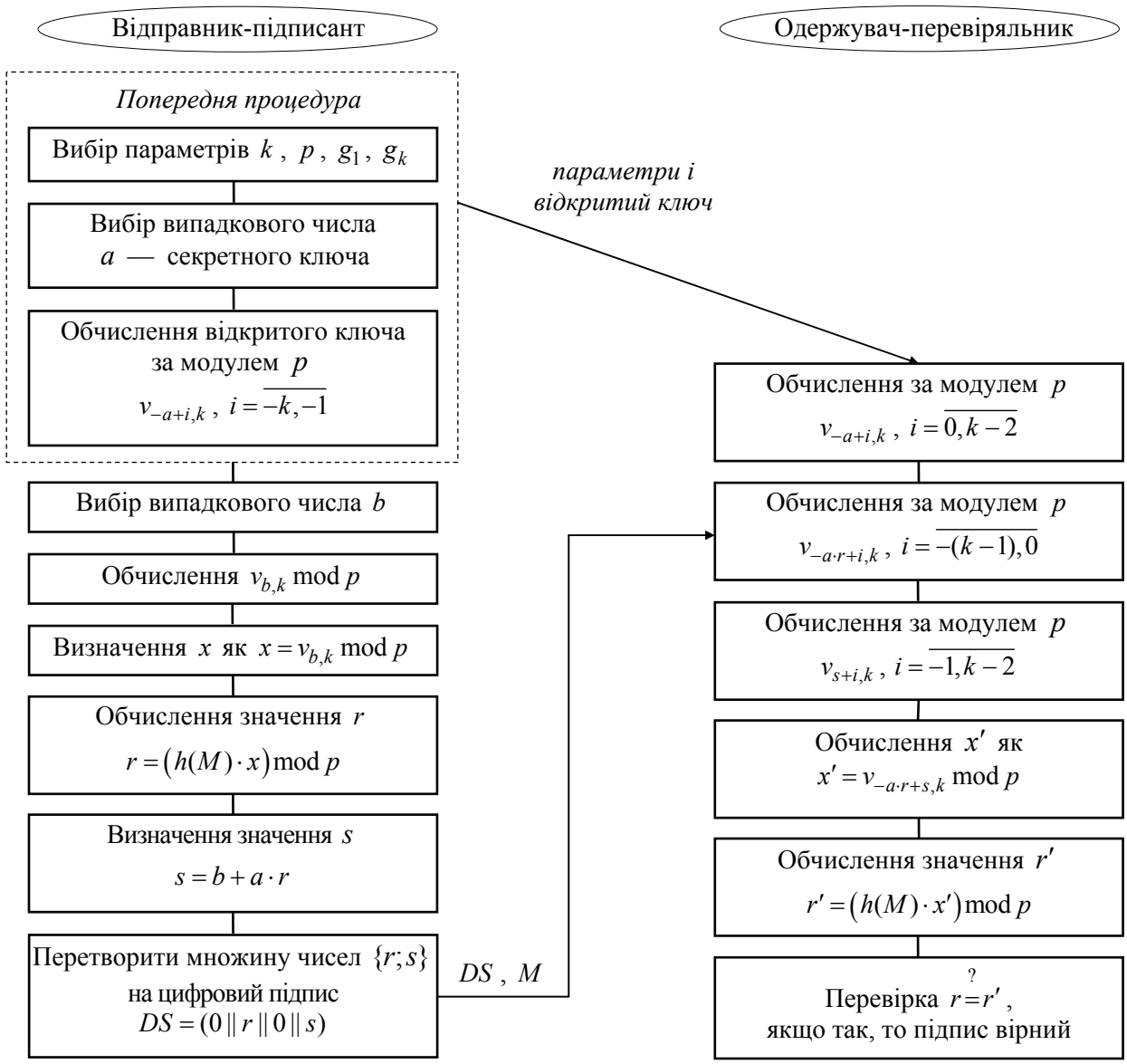

Схема цифрового підписування на основі елементів V_k-послідовності

Операція за модулем в схемі цифрового підписування використовується для обмеження розрядності чисел під час виконання арифметичних операцій.

Обчислення елемента $v_{b,k} \bmod p$ відправник може виконати попередньо, заздалегідь до безпосереднього формування цифрового підпису з повідомлення M.

В запропонованому методі цифрового підписування основні обчислення виконуються згідно із залежністю (3). Обчислення елемента $v_{n+m,k}$ згідно з цією залежністю здійснюється на основі елементів $v_{n+i,k}$, $i=\overline{-(k-1),0}$ та елементів $v_{m+i,k}$, $i=\overline{-1,k-2}$.

В разі необхідності отримання певного послідовного набору елементів V_k-послідовності у кількості, більшій ніж k, достатньо отримати будь-які послідовні k з них, оскільки інші можуть бути обчислені згідно з формулами (1) або (2) на основі вже отриманих.

Також одержувачу слід виконувати обчислення елементів $v_{-a\cdot r+i,k}$, $i=\overline{-(k-1),0}$, які можна здійснювати згідно з представленим в роботі [7] методом обчислення елементів $v_{-m\cdot n,k}$.

Визначивши, як можуть отримуватись елементи V_k-послідовності, що використовуються згідно із запропонованою можливістю цифрового підписування, отримаємо такий протокол цифрового підписування.

П. 1. Задати параметр k.

П. 2. Вибрати p.

П. 3. Вибрати g_1, g_k.

П. 4. Відправнику передати параметри Одержувачу.

П. 5. Відправнику вибрати випадкове число a — секретний ключ.

П. 6. Відправнику обчислити відкритий ключ за модулем p $v_{-a+i,k}$, $i=\overline{-k,k-2}$, використовуючи алгоритм прискореного обчислення елементів $v_{n,k}$ для від'ємних значень n.

П. 7. Відправнику передати відкритий ключ $v_{-a+i,k} \bmod p$, $i=\overline{-k,-1}$, Одержувачу.

П. 8. Одержувачу обчислити за модулем p $v_{-a+i,k}$, $i=\overline{0,k-2}$ за формулою (1).

П. 9. Відправнику вибрати випадкове число b.

П. 10. Відправнику обчислити $v_{b,k} \bmod p$, використовуючи алгоритм прискореного обчислення елементів $v_{n,k}$ для додатних значень n.

П. 11. Відправнику визначити x як $x = v_{b,k} \bmod p$.

П. 12. Відправнику обчислити значення r як $r = \left(h(M)\cdot x\right) \bmod p$ за допомогою обраної функції хешування h від повідомлення M.

П. 13. Відправнику визначити значення s як $s = b + a \cdot r$.

П. 14. Відправнику перетворити множину цілих чисел $\{r; s\}$ у цифровий підпис вигляду $DS = \left(0 \| r \| 0 \| s\right)$ і передати його разом з повідомленням M Одержувачу.

П. 15. Одержувачу обчислити за модулем p $v_{-a\cdot r+i,k}$, $i=\overline{-(k-1),0}$, використовуючи алгоритм прискореного обчислення елементів $v_{-m\cdot n,k}$.

П. 16. Одержувачу обчислити за модулем p елементи $v_{s+i,k}$, $i=\overline{-1,k-2}$, використовуючи алгоритм прискореного обчислення елементів $v_{n,k}$ для додатних значень n.

П. 17. Одержувачу обчислити $x' = v_{-a\cdot r+s,k} \bmod p$ згідно із залежністю (3).

П. 18. Одержувачу обчислити значення r' як $r' = \left(h(M)\cdot x'\right) \bmod p$.

П. 19. Одержувачу перевірити, чи виконується $r \overset{?}{=} r'$, якщо так, то підпис вважати вірним.

У п. 2 проводиться вибір параметра p, який є модулем під час обчислень в представленому протоколі та визначає верхню межу діапазону чисел, що отримуються під час цих обчислень.

У п. 3 відбувається вибір параметрів g_1, g_k. Оскільки значення будь-якого числа в розробленому протоколі обмежується параметром p, вказані параметри слід вибирати в діапазоні $[1, p-1]$. При цьому вибір можна здійснювати за допомогою будь-якого генератора випадкових чисел у вказаному діапазоні.

У п. 10 протоколу цифрового підписування відправнику необхідно здійснювати обчислення $v_{b,k} \bmod p$, а у п. 16 одержувачу необхідно здійснювати обчислення за модулем p елементів $v_{s+i,k}$, $i=\overline{-1,k-2}$. Ці обчислення можна здійснювати за одним з алгоритмів прискореного обчислення елементів $v_{n,k}$ для додатних n, які викладено в роботі [6].

Так само можна здійснювати обчислення за модулем p елементів $v_{-a+i,k}$, $i=\overline{-k,k-2}$, що виконуються у п. 6 протоколу цифрового підписування, на основі одного з запропонованих у тій самій роботі [6] алгоритмів прискореного обчислення елементів $v_{n,k}$ для від'ємних n.

У п. 15 одержувачу необхідно обчислювати за модулем p елементи $v_{-a\cdot r+i,k}$, $i=\overline{-(k-1),0}$. Для цього можна використати алгоритм прискореного обчислення елементів $v_{-m\cdot n,k}$, описаний в роботі [7].

Аналіз криптографічної стійкості запропонованого методу цифрового підписування показав, що його стійкість знаходиться приблизно на тому ж рівні, принаймні є не меншою, ніж у відомих анало-

гів. Так само аналіз обчислювальної складності запропонованого методу показав, що він в цілому має приблизно такий самий рівень обчислювальної складності, як і відомі аналоги.

При цьому запропонований метод на основі V_k -послідовностей має дві переваги перед відомими методами як щодо стійкості, так і щодо обчислювальної складності. По-перше, в запропонованому методі є можливість змінювати параметр k , що, в свою чергу, дає можливість підвищувати криптостійкість за рахунок збільшення складності виконання протоколу цифрового підписування. По-друге, запропонований метод у порівнянні з відомими аналогами має значно простішу процедуру задання параметрів, оскільки їх вибір не потребує проведення складних обчислень над великими числами.

Однак важливою перевагою запропонованого методу на основі V_k -послідовностей є те, що за необхідності процедуру перевірки підпису можна значно спростити, якщо обчислення елементів $v_{s+i,k} \bmod p$, $i = \overline{-1, k-2}$, здійснювати не одержувачу, а відправнику, і передавати потім ці елементи перевіряльнику замість індексу s (заявка на корисну модель № u 2013 06324 від 22.05.2013 р.). Тоді відправнику необхідно буде передавати більшу кількість чисел і виконувати три обчислення елементів V_k -послідовності за прискореним алгоритмом замість двох. Однак такий варіант методу буде мати дві суттєвих переваги, по-перше, підвищиться стійкість методу, оскільки тепер зловмиснику замість індексу s буде відомий набір елементів $v_{s,k} \bmod p$, обчислених за цим індексом, і, по-друге, значно спроститься процедура перевірки підпису, оскільки в такому випадку одержувачу необхідно буде виконувати лише одне обчислення елементів V_k -послідовності за прискореним алгоритмом.

Висновки

Показано можливість цифрового підписування на основі математичного апарату рекурентних V_k -послідовностей, а також представлено протокол реалізації такої можливості.

Аналіз криптографічної стійкості та обчислювальної складності показав, що в цілому криптографічна стійкість і обчислювальна складність запропонованої можливості цифрового підписування знаходяться приблизно на тому ж рівні, що і у відомих аналогів, але при цьому запропонований метод за певних умов дозволяє значно спрощувати обчислення процедури перевірки підпису, а також підвищувати стійкість всього процесу цифрового підписування.

Крім того, запропонований метод дозволяє змінювати стійкість методу залежно від параметра *k*-порядку послідовності, а також має простішу процедуру задання параметрів у порівнянні з відомими аналогами.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Романец Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеева, В. Ф. Шаньгин. — М. : Радио и связь, 2001. — 376 с.

2. Menezes A. J. Handbook of Applied Cryptography / A. J. Menezes, P. C. van Oorschot, S. A. Vanstone. — CRC Press, 2001. — 816 p.

3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. — М. : Триумф, 2002. — 816 с.

4. Молдавян Н. А. Теоретический минимум и алгоритмы цифровой подписи / Н. А. Молдавян. — СПб. : БХВ-Петербург, 2010. — 304 с.

5. Rivest R. L. A method for obtaining digital signatures and public-key cryptosystems / R. L. Rivest, A. Shamir, L. M. Adleman // Communications of the ACM. — 1978. — V. 21. — Pp. 120—126.

6. Яремчук Ю. Є. Розробка алгоритмів прискореного обчислення елементів рекурентних послідовностей для криптографічних застосувань / Ю. Є. Яремчук // Реєстрація, зберігання і обробка даних.. — 2013. — Т. 15, № 1. — С. 14—22.

7. Яремчук Ю. Є. Методи автентифікації на основі рекурентних послідовностей / Ю. Є. Яремчук // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — 2013. — Вип. 1(25). — С. 39—49.

Рекомендована кафедрою менеджменту та безпеки інформаційних систем

Стаття надійшла до редакції 23.09.2013
Рекомендована до друку 3.10.2013

Яремчук Юрій Євгенович — професор кафедри менеджменту та безпеки інформаційних систем.
Вінницький національний технічний університет, Вінниця